

IN THE CLAIMS

Claims 2, 9, 11-12, 15-19, 23-25, 27, 29-35, and 41-43 are amended. Claims 44-45 are added.

1 1. (Original) A method of examining a network, including:  
2 identifying an operating system of a remote host, including a version and a  
3 patch level of the operating system;  
4 identifying a service of the remote host, including a version and a patch level  
5 of the service; and  
6 identifying a vulnerability of the network based on information obtained from  
7 the steps of identifying an operating system and identifying a service.

1 2. (Currently Amended) The method of claim 1, wherein:  
2 the step of identifying an operating system includes sending a first set of  
3 packets to the remote host and receiving a second set of packets from  
4 the remote host in response to said first set of packets;  
5 the step of identifying a service includes sending a third set of packets to the  
6 remote host and receiving a fourth set of packets from the remote host  
7 in response to said third set of packets, wherein information contained  
8 in said third set of packets on information received in said second set  
9 of packets; and  
10 the step of identifying a vulnerability includes comparing information  
11 contained in the second set of packets and the fourth set of packets to  
12 preexisting information in a database.

1 3. (Original) The method of claim 1, wherein the step of identifying  
2 an operating system includes sending three sets of packets to the remote host and  
3 receiving three respective sets of responsive packets from the remote host.



1 4. (Original) A method of examining a network, including:  
2 nonintrusively and reliably identifying an operating system of a remote host  
3 including identifying a version of the operating system;  
4 nonintrusively and reliably identifying a service of the remote host including  
5 identifying a version of the service.

1 5. (Original) The method of claim 4, further including:  
2 identifying a vulnerability of the network.

1 6. (Original) The method of claim 4, further including:  
2 identifying a trojan application on the host.

1 7. (Original) The method of claim 4, further including:  
2 identifying unauthorized software use on the host.

1 8. (Original) The method of claim 4, further including:  
2 identifying security policy violations on the network.

1 9. (Currently Amended) The method of claim 4, wherein:  
2 the step of identifying an operating system further includes identifying a patch  
3 level of the operating system; and  
4 the step of identifying a service further includes identifying a patch level of  
5 the service.

1 10. (Original) The method of claim 4, wherein the steps of identifying  
2 an operating system and identifying a service each includes:  
3 sending a selected packet to the remote host;  
4 receiving from the remote host a reflexive responsive packet.



1 11. (Currently Amended) The method of claim 4, wherein the steps of  
2 identifying an operating system and identifying a service each includes:  
3 sending a plurality of selected packets to the remote host; and  
4 receiving from the remote host a plurality of reflexive responsive packets.

1 12. (Currently Amended) The method of claim 4, wherein:  
2 the step of identifying an operating system includes sending a first set of  
3 packets to the remote host and receiving a second set of packets from  
4 the remote host in response to said first set of packets; and  
5 the step of identifying a service includes sending a third set of packets to the  
6 remote host and receiving a fourth set of packets from the remote host  
7 in response to said third set of packets.

a1  
1 13. (Original) A method of examining a network, including:  
2 identifying an operating system of a remote host including identifying a  
3 version of the operating system;  
4 identifying a service of the remote host including identifying a version of the  
5 service, and  
6 identifying a vulnerability of the network.

1 14. (Original) The method of claim 13, wherein:  
2 the step of identifying a vulnerability includes using information obtained  
3 from the steps of identifying an operating system and identifying a  
4 service to identify the vulnerability.

1 15. (Currently Amended) The method of claim 13, wherein:  
2 the step of identifying an operating system further includes identifying a patch  
3 level of the operating system; and  
4 the step of identifying a service includes identifying a patch level of the  
5 service.



1 16. (Currently Amended) The method of claim 13, wherein the steps  
2 of identifying an operating system, identifying a service, and identifying a vulnerability  
3 each includes:

4 sending a selected packet to the remote host; and  
5 receiving from the remote host a reflexive responsive packet.

1 17. (Currently Amended) The method of claim 13, wherein:  
2 the step of identifying an operating system includes sending a first set of  
3 packets to the remote host and receiving a second set of packets from  
4 the remote host in response to said first set of packets;  
5 the step of identifying a service includes sending a third set of packets to the  
6 remote host and receiving a fourth set of packets from the remote host  
7 in response to said third set of packets; and  
8 the step of identifying a vulnerability includes comparing information  
9 contained in the second set of packets and the fourth set of packets to  
10 information in a database.

1 18. (Currently Amended) The method of claim 17, wherein:  
2 information contained in said third set of packets is based on information  
3 received in said second set of packets; and  
4 information contained in said fifth set of packets is based on information  
5 received in said fourth set of packets.

1 19. (Currently Amended) A method of examining a network,  
2 including:  
3 sending a set of selected packets to a host on the network;  
4 receiving from the remote host a set of reflexive responsive packets; and  
5 identifying conditions of the remote host by using information received in the  
6 reflexive responsive packets, wherein the conditions include an  
7 operating system of the host, and a service of the host.



1                   20.   (Original) The method of claim 19, whercin the conditions further  
2 include a vulnerability of the host.

1                   21.   (Original) The method of claim 19, wherein the conditions further  
2 include the presence of unauthorized software.

1                   22.   (Original) The method of claim 19, wherein the conditions include  
2 the presence of a trojan application.

1                   23.   (Currently Amended) The method of claim 19, wherein:  
2 identifying an operating system includes identifying a version; and  
3 identifying a service includes identifying a version.

a!  
1                   24.   (Currently Amended) The method of claim 19, wherein:  
2 identifying an operating system includes identifying a version and a patch  
3 level; and  
4 identifying a service includes identifying a version and a patch level.

1                   25.   (Currently Amended) The method of claim 19, wherein  
2 the step of sending a set of selected packets to a host on the network includes  
3 sending a plurality of sets of packets to the host; and  
4 the step of receiving from the remote host a set of reflexive responsive packets  
5 includes receiving a like plurality of sets of reflexive responsive  
6 packets.

1                   26.   (Original) A method of detecting a vulnerability of a network,  
2 comprising:  
3 sending a first set of selected packets to a host on the network;  
4 receiving a second set of packets from the remote host in response to the first  
5 set of packets;



6 sending a third set of selected packets to a host on the network, wherein  
7 information contained in the third set of packets is based on  
8 information contained in the second set of packets;  
9 receiving a fourth set of packets from the remote host in response to the third  
10 set of packets;  
11 sending a fifth set of selected packets to a host on the network, wherein  
12 information contained in the fifth set of packets is based on  
13 information contained in the fourth set of packets;  
14 receiving a sixth set of packets from the remote host in response to the fifth  
15 set of packets;  
16 based on information contained in the second, fourth, and sixth set of packets,  
17 identifying a operating system of a host on the network, including a  
18 version and a patch level.

a1  
1 27. (Currently Amended) The method of claim 26, further including:  
2 sending a seventh set of selected packets to a host on the network;  
3 receiving an eighth set of packets from the remote host in response to the  
4 seventh set of packets;  
5 sending a ninth set of selected packets to a host on the network;  
6 receiving a tenth set of packets from the remote host in response to the ninth  
7 set of packets; and  
8 based on information contained in the eight and tenth sets of packets,  
9 identifying a service of a host on the network, including a version and  
10 a patch level.

1 28. (Original) The method of claim 27, further including:  
2 based on information contained in at least the tenth sequence, identifying a  
3 vulnerability.

1 29. (Currently Amended) The method of claim 26, wherein:  
2 the first set of packets includes:  
3 a SYN Packet with false flag in the TCP option header;



4 a Fragmented UPD packet with malformed header (any header  
5 inconsistency is sufficient), where the packet is 8K in size;  
6 a FIN Packets of a selected variable size or a FIN packet without the  
7 ACK or SYN flag properly set; and  
8 a generic, well-formed ICMP ECHO request packet;  
9 the third set of packets includes:  
10 a generic well-formed TCP Header set to 1024 bytes in size;  
11 a Packet requesting an ICMP Timestamp;  
12 a Packet with min/max segment size set to a selected variable value;  
13 and  
14 a UPD packet with the fragment bit set;  
15 the fifth set of packets includes:  
16 a TCP Packet with the header and options set incorrectly;  
17 a well-formed ICMP Packet;  
18 a Fragmented TCP or UPD packet;  
19 a packet with an empty TCP window or a window set to zero;  
20 a generic TCP Packet with 8K of random data; and  
21 a SYN Packet with ACK and RST flags set.

1 30. (Currently Amended) A method of examining a network,  
2 comprising:  
3 sending a plurality of packets to a network;  
4 receiving a responsive plurality of packets from the network;  
5 comparing information in the responsive packets to information stored in a  
6 database; and  
7 based on the comparison, identifying a plurality of network conditions,  
8 including a vulnerability of the network.

1 31. (Currently Amended) A method of examining a network,  
2 comprising:  
3 sending packets to a network;



4 receiving responsive packets from the network;  
5 comparing information in the responsive packets to information stored in a  
6 database; and  
7 based on the comparison, identifying a trojan application on the network.

1 32. (Currently Amended) A method of examining a network,  
2 comprising:  
3 sending packets to a network;  
4 receiving responsive packets from the network;  
5 comparing information in the responsive packets to information stored in a  
6 database; and  
7 based on the comparison, identifying unauthorized software use on the  
8 network.

a  
1 33. (Currently Amended) A method of examining a network,  
2 comprising:  
3 sending packets to a network;  
4 receiving responsive packets from the network;  
5 comparing information in the responsive packets to information stored in a  
6 database; and  
7 based on the comparison, inferring an unknown vulnerability.

1 34. (Currently Amended) A method of examining a network,  
2 comprising:  
3 sending packets to a network;  
4 receiving responsive packets from the network;  
5 comparing information in the responsive packets to information stored in a  
6 database; and  
7 based on the comparison, identifying a security policy violation.



1 35. (Currently Amended) A system for examining a network,  
2 comprising:  
3 a database including a set of reflex signatures;  
4 a packet generator;  
5 a comparison unit in communication with the packet generator and the  
6 database;  
7 wherein the packet generator is designed to generate and transmit a plurality  
8 of test packets to the network; and  
9 wherein the comparison unit is designed to receive responsive packets from  
10 the network and to compare responsive packet information with the  
11 reflex signatures.

a  
1 36. (Original) The system of claim 35, wherein the comparison unit is  
2 further designed to identify a vulnerability in the network based on its comparison of  
3 packet information with reflex signatures.

1 37. (Original) The system of claim 35, wherein the comparison unit is  
2 further designed to identify an operating system type, version, and patch level and a  
3 service type, version, and patch level of a host on the network.

1 38. (Original) The system of claim 35, wherein the comparison unit is  
2 designed to provide information to the packet generator, and wherein the packet  
3 generator is designed to use the information to selectively generate packets.

1 39. (Original) A computer readable medium, having instructions  
2 stored therein, which, when executed by a computer, causes the computer to perform the  
3 steps of:  
4 identifying an operating system of a remote host, including a version of the  
5 operating system;  
6 identifying a service on the port and a service of the remote host, including a  
7 version of the service; and



8 identifying a vulnerability of the network-based on information obtained from  
9 the steps of identifying an operating system and identifying a service.

1 40. (Original) The computer readable medium of claim 39, wherein:  
2 the instructions for identifying an operating system further include  
3 instructions for identifying a patch level of the operating system; and  
4 the instructions for identifying a service further include instructions for  
5 identifying a patch level of the service.

1 41. (Currently Amended) The computer readable medium of claim 39,  
2 wherein:  
3 the step of identifying an operating system includes sending a first set of  
4 packets to the remote host and receiving a second set of packets from  
5 the remote host in response to said first set of packets;  
6 the step of identifying a service includes sending a third set of packets to the  
7 remote host and receiving a fourth set of packets from the remote host  
8 in response to said third set of packets, wherein information contained  
9 in said third set of packets is based on information received in said  
10 second set of packets; and  
11 the step of identifying a vulnerability includes comparing information  
12 contained in the second sequence of packets and the fourth sequence  
13 of packets to information in a database.

1 42. (Currently Amended) A method for use by a host on a network,  
2 comprising:  
3 receiving a set of selected packets from remote equipment; and  
4 automatically sending a second set of packets to said remote equipment,  
5 which packets include information that enables the remote equipment  
6 to identify a vulnerability on the network.



1 43. (Currently Amended) A method for use by a host on a network,  
2 comprising:  
3 receiving a first set of packets from remote equipment;  
4 automatically sending a second set of packets to said remote equipment;  
5 receiving a third set of packets from the remote equipment;  
6 automatically sending a fourth set of packets to the remote equipment;  
7 receiving a fifth set of packets from the remote equipment;  
8 automatically sending a sixth set of packets from the remote equipment;  
9 receiving a seventh set of packets from remote equipment;  
10 automatically sending an eighth set of packets from the remote equipment;  
11 receiving a ninth set of packets from the remote equipment; and  
12 automatically sending a tenth set of packets from the remote equipment;  
13 wherein said second, fourth, and sixth sets of packets include information that  
14 enables the remote equipment to identify an operating system on the  
15 network, including a version and a patch level;  
16 wherein said eighth and tenth sets of packets include information that enables  
17 the remote equipment to identify a service, including a version and a  
18 patch level.

1 44. (New) A method of examining a network, including:  
2 identifying an operating system of a remote host, including a version and a  
3 patch level of the operating system with a first set of packets, the first  
4 set of packets comprising an operating system packet to determine the  
5 operating system, an operating system version packet to determine the  
6 operating system version based on the determined operating system,  
7 and an operating system patch level packet to determine the operating  
8 system patch level based on the determined operating system version;  
9 identifying a service of the remote host, including a version and a patch level  
10 of the service with a second set of packets based on at least one of the  
11 first set of packets, the first set of packets comprising a service packet



12 to determine the service, a service version packet to determine the  
13 service version based on the determined service, and a service patch  
14 level packet to determine the service patch level based on the  
15 determined service version; and  
16 identifying a vulnerability of the network based on information obtained from  
17 the steps of identifying an operating system and identifying a service.

45. (New) A method of examining a network, including:  
identifying an operating system of a remote host, including a version and a  
patch level of the operating system, with responses to nonconforming  
data packets;  
identifying a service of the remote host, including a version and a patch level  
of the service with responses to nonconforming data packets; and  
identifying a vulnerability of the network based on information obtained from  
the steps of identifying an operating system and identifying a service.